Congruence Modulo p

Let p be an integer greater than 1. Then we define a corresponding binary relation on the integers as follows.

We say that m is *congruent to* n *modulo* p, and write $n \equiv m(\text{mod } p)$, if $m - n$ is an integer multiple of p.

For example, take $p = 3$. Then 1 is congruent to 4 modulo p, but not congruent to 3.

Let R_p be the set

$$\{(m, n) \ : \ m \equiv n(\text{mod } p)\}.$$

Is the relation R_p reflexive?

Is it transitive?

Is it symmetric?

The answer to all three questions is yes, and hence each relation R_p is an equivalence relation on the integers.

An Equivalence Relation on Strings

Let Σ be an alphabet. We define a binary relation $\sim$ on Σ^* as follows:

$$v \sim w \text{ if and only if } |v| = |w|.$$

The relation $\sim$ is an equivalence.

Reflexivity. We have $|w| = |w|$, and hence $w \sim w$, for all strings w.

Symmetry. If $v \sim w$, then by definition $|v| = |w|$. By the symmetry of equality we thus have $|w| = |v|$, and hence $w \sim v$.

Transitivity. Suppose $u \sim v$ and $v \sim w$. Then $|u| = |v|$ and $|v| = |w|$ and therefore, by the transitivity of equality, $|u| = |w|$, which implies $u \sim w$.

Let Σ^k be the set of all strings of size k over Σ.

The collection of all sets Σ^k, $k \in \mathbb{N}$, is a partition of Σ^*. In fact, the sets Σ^k are the equivalence classes induced by $\sim$.

Equinumerous Sets

Two sets A and B are said to be *equinumerous* (or of the same size) if, and only if, there is a bijection from A to B. (Recall that a function is a bijection if it is one-to-one and onto.)

We write $A \sim B$ if A and B are of the same size in this sense. The relation $\sim$ is also an equivalence.

Reflexivity. The identity function on A is a bijection from A to A, thus $A \sim A$.

Symmetry. If there is a bijection f from A to B, then the inverse function f^-1 is a bijection from B to A. THus, $A \sim B$ implies $B \sim A$.

Transitivity. Suppose $A \sim B$ and $B \sim C$. Then there are bijections f from A to B and g from B to C. The composition of the two functions f and g is a bijection from A to C and thus $A \sim C$.

Finite and Infinite Sets

We call a set *finite* if it is equinumerous with some set $\{0, 1, \ldots, n-1\}$, for some natural number n.

If A is equinumerous with n, then it is said to be of *cardinality* n, written $|A| = n$.

If a set is not finite, it is called *infinite*.

Examples of infinite sets are the sets of natural numbers, of integers, of rational numbers, of real numbers. But not all of these sets are equinumerous, as we shall see!

A set is called *countably infinite* if it is equinumerous with the set $\mathbf{P}$ of positive natural numbers.

The set of natural numbers is countably infinite as the function f, defined by $f(n) = n + 1$, is a bijection from $\mathbf{N}$ to $\mathbf{P}$.

A set is called *countable* if it is finite or countably infinite; and *uncountable* otherwise.

Informally, one can list the elements of a countable set, though the list may never end.

Examples of Countable Sets

The set of integers $\mathbf{Z}$ is countable. A suitable bijection from $\mathbf{Z}$ to $\mathbf{P}$ is the function f, defined by:

$$f(n) = \begin{cases} 2n + 1 & \text{if } n \geq 0 \\ -2n & \text{if } n < 0 \end{cases}$$

Surprisingly, the set of rational numbers $\mathbf{Q}$ is also countable.